THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
ASHEVILLE DIVISION

TERRA WEAVER and DAVID LE, individually and on behalf of all others similarly situated, *Plaintiffs*, v. EQUIFAX, INC., *Defendant.*	CASE NO. **PLAINTIFFS' CLASS ACTION COMPLAINT**

Plaintiffs Terra Weaver and David Le (hereinafter, collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, allege the following against Equifax, Inc. ("Equifax"):

NATURE OF THE CASE

1) This case stems from the widely-publicized data breach caused by Defendant Equifax's failure to secure and safeguard consumers' personally identifiable information ("PII"). As part of its usual business practices as a consumer credit reporting agency ("CRA"), Equifax collects from various sources PII on millions of Americans.

2) On September 7, 2017, Equifax publicly announced a cybersecurity incident that resulted in the unauthorized disclosure of PII potentially impacting approximately 143 million U.S. consumers (the "Data Breach"). The Data Breach was caused by cyberattackers exploiting a website application vulnerability that allowed them to

gain access to files containing PII. Equifax admitted the Data Breach occurred from mid-May through July 2017 and provided unauthorized access to PII primarily including names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. Equifax also admitted that approximately 209,000 U.S. consumers' credit card numbers were accessed. Equifax has known about the Data Breach since July 29, 2017, but delayed notifying the public for several weeks and has yet to provide an explanation for this delay.

3) Through the use of customary and routine data security methods, Equifax could have and should have prevented the unauthorized disclosure of the PII of millions of Americans. As a result of Equifax's negligence and unlawful conduct millions of Americans, including the Plaintiffs, are now subject to the threat of having their identities stolen and this PII is now readily available to cybercriminals for misuse. Through Equifax's lax security practices that diverge from the practices of other CRAs, the rights of Plaintiffs and the Class in the protection of their PII has been violated.

4) As a result of the Equifax Data Breach, and Equifax's intentional, illegal, and negligent conduct, Plaintiffs and/or the putative Class members are likely to suffer the following:

a. unauthorized use of their PII;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their PII;

e. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft protection services, and the stress, nuisance and annoyance of dealing with all issues resulting from the Equifax Data Breach;

g. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII being placed in the hands of criminals and already misused via the sale of Plaintiffs' and Class members' information on the Internet black market;

h. damages to and diminution in value of their PII entrusted to Equifax for the sole purpose of purchasing products and services from Equifax; and

i. the loss of Plaintiff's and Class members' privacy.

5) The aforementioned injuries are the direct and proximate result of the Data Breach caused by Equifax's wanton failure to implement or maintain adequate data security measures for PII.

6) Plaintiffs now seek a remedy for the harms caused by Equifax's conduct that lead to the Data Breach. Plaintiffs assert common law claims of negligence and violations of the Fair Credit Reporting Act ("FCRA") and state consumer protection statutes. Plaintiffs also seek reimbursement of out-of-pocket losses, other compensatory damages, further and more robust credit monitoring services with accompanying identity theft insurance, and injunctive relief including an order requiring Equifax to implement improved data security measures.

JURISDICTION AND VENUE

7) This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs and there are millions of putative class members, some of whom do not have the same citizenship as Equifax.

8) This Court may exercise personal jurisdiction over Equifax as Equifax does business in this jurisdiction and maintains sufficient minimum contacts within this jurisdiction to satisfy the Constitutional requirements of this Court exercising jurisdiction over it.

9) Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

PARTIES

10) Plaintiff Terra Weaver is a resident of Buncombe County, North Carolina. She has spent time and resources monitoring her credit and finances and reasonably believes her PII was compromised in the Data Breach.

11) Plaintiff David Le is a resident of Buncombe County, North Carolina. He has spent time and resources monitoring his credit and finances and reasonably believes his PII was compromised in the Data Breach.

12) Defendant Equifax, Inc. is a Delaware corporation with its principal place of business located at 1550 Peachtree Street NE, Atlanta, Georgia 30309. Equifax, Inc. may be served through its registered agent, Shawn Baldwin, at its principal office address identified above.

STATEMENT OF FACTS

A. Background on Data Breach

13) Equifax is one of three nationwide credit-reporting agencies under FCRA (a "CRA") and its principal business is tracking and rating the financial history and credit of U.S. consumers. Equifax generates reports on these consumers that are used by financial institutions to determine the credit-worthiness of potential customers. CRAs like Equifax obtain information on consumers including the following: lines of credit, mortgage information, child support payments, utility payments, rent payments, and addresses and contact information of employers. CRAs use this compiled information to create "credit scores" for consumers, which are used by the financial industry and others in determining whether to extend credit, loans, and services to U.S. consumers.

14) At all relevant times, Equifax maintained a publicly available website at www.equifax.com. Within that website are various publicly available web pages directed to consumers and the general public. Among those web pages is one through which Equifax invites consumers and the public to submit information to initiate and support a formal dispute of information in their credit reports.

15) At all relevant times, Equifax promised the public that safeguarding consumers' sensitive, personal information is "a top priority."

16) At all relevant times on its Privacy Policy, available through a hyperlink at the bottom of each page of its public website, Equifax represented to the public:

> We have built our reputation on our commitment to deliver reliable information to our customers (both businesses and consumers) and to protect the privacy and confidentiality of personal information about consumers. We also protect the sensitive information we have about businesses. Safeguarding the privacy and security of information, both online and offline, is a top priority for Equifax.

17) Equifax likewise represented to consumers that it would keep all of their credit information, including that which consumers submitted through the Dispute Portal, secure. In its "Consumer Privacy Policy for Personal Credit Reports," accessible at http://www.equifax.com/privacy/personal-credit-reports, Equifax represented that it has "reasonable, physical, technical and procedural safeguards to help protect your [i.e. consumers'] personal information."

18) Because Equifax may obtain information on consumers who may not otherwise have a direct business relationship with Equifax, Equifax maintains PII on consumers that consumers did not affirmatively give Equifax. Additionally, Equifax may maintain PII

on individuals that Equifax does not provide directly with services or products. This makes the present Data Breach different from other high-profile data security breaches in the past in that consumers affected by the Data Breach did not voluntarily provide information to Equifax.

19) Equifax issued the first public disclosure of the Data Breach on September 7, 2017 (the "Data Breach Announcement"). A copy of this Data Breach Announcement is attached hereto as Exhibit A. According to the Data Breach Announcement, Equifax discovered the Data Breach on July 29th. According to Equifax, cyberattackers "exploited a U.S. website application vulnerability to gain access to certain files." According to the Data Breach Announcement, "[b]ased on [Equifax's] investigation, the unauthorized access occurred from mid-May through July 2017."

20) "The information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed." This type of data should have received extra protection, not substandard protection that would allow cyberattackers to access this information through a simple "website application."

21) PII like that described in the foregoing paragraph is extremely valuable to certain criminal elements that may use phishing tactics and other technologies to steal the identity of individuals or open and use credit lines in the names of other individuals. At all relevant times, Equifax was well aware, or reasonably should have been aware, that the PII collected, maintained and stored in the POS systems is highly sensitive,

susceptible to attack, and could be used for wrongful purposes, such as identity theft and fraud, by third parties.

22) In other words, the PII of Plaintiffs and Class members is private and sensitive in nature and Equifax failed to adequately protect this information from unauthorized disclosure. Equifax did not obtain Plaintiffs' and Class members' consent to disclose their PII to any cyberattacker or any person not authorized to hold such information as required by applicable law and industry standards.

23) Many high-profile data breaches have affected millions of people and these data breaches have been the subject of numerous media reports that have made it generally well known that PII like that stolen from Equifax is highly coveted and a frequent target of cyberattackers. Despite the frequent public announcements concerning data breaches caused by corporations failing to properly protect important PII, Equifax maintained an insufficient and inadequate system to protect the PII of Plaintiffs and Class members. PII is a valuable commodity because a black market exists in which criminals and cyberattackers openly post or sell stolen social security numbers and other personal information on a number of websites on the dark Internet. PII can be used to open new financial accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.

24) At all relevant times, Equifax knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if cyberattackers gained access to its data systems. In fact, shortly following the Data Breach Announcement, Equifax's former CEO, Rick Smith, issued a public statement

in which he acknowledged that Equifax's Data Breach "impacted those who rely upon us to protect their personal information." In other words, Equifax knows that individuals have a right and an expectation that the information Equifax holds about them should be protected from cyberattacks. Former CEO Smith went on to further claim that Equifax has "more to do" on protecting against cyberattacks.

25) In the Data Breach Announcement, former CEO Smith further stated that "This is clearly a disappointing event for our company, and one that strikes at the heart of who we are and what we do. I apologize to consumers and our business customers for the concern and frustration this causes."

26) Unfortunately for consumers, Equifax's approach to cybersecurity was at the very least negligent and more likely lackadaisical, reckless, and unlawful and the ramifications of Equifax's failure to keep Plaintiffs' and Class members' data secure are severe.

27) On September 13, 2017, Equifax provided an update as to the source of the data breach. According to Equifax, "Equifax has been intensely investigating the scope of the intrusion with the assistance of a leading, independent cybersecurity firm to determine what information was accessed and who has been impacted. We know that criminals exploited a U.S. website application vulnerability. The vulnerability was Apache Struts CVE-2017-5638." Apache Struts is an open-source software used across the corporate world to provide web applications in Java, and it powers front- and back-end applications, including Equifax's public website.

28) According to certain security experts, "The Apache flaw was first spotted around March 7, 2017, when security firms began warning that attackers were actively

exploiting a 'zero day' vulnerability in Apache Struts." Zero day refers to software or hardware flaws that cyberattackers find and figure out how to use for commercial or personal gain before the vendor even knows about the flaws. The following day, March 8, 2017, Apache had released new versions of the software to mitigate the vulnerability. If this is the source of the vulnerability that lead to the Data Breach, this means that Equifax operated with this known vulnerability on its U.S. web application for months prior to the Data Breach and a simple update of this widely used open-source software could have prevented the Data Breach altogether. If this is the source of the Data Breach, Equifax's failure to timely implement this patch to this vulnerability is a gross deviation of the standard of care Equifax owed to the Plaintiffs and Class Members to protect their PII that Equifax had collected.

29) In other words, from at least March 7, 2017, through July 30, 2017, Equifax left at least 143 million consumers' sensitive and private information exposed and vulnerable to intruders by relying on open-source code that it knew or should have known was insecure and subject to exploitation. Although patches, workarounds, and other fixes for the vulnerability were available and known – or at least should have been known – to Equifax as of March 7, 2017, Equifax failed to avail itself of these remedies or employ other security controls that could have protected the security of the PII collected and stored by Equifax.

30) There are, and at all relevant times have been, multiple well-known resources available to support companies relying on open-source code, including Apache Struts. These resources publicly announce to users when security vulnerabilities in the

open-source code are discovered and verified, including in Apache Struts, compare the associated risks of such vulnerabilities, and propose fixes.

31) For example, the Apache Software Foundation ("Apache"), a non-profit corporation, releases updated versions of Apache Struts to "patch" it against verified security vulnerabilities. Apache also releases Security Bulletins on its website regarding security flaws in Apache Struts, noting the nature of the vulnerability and ways to resolve it. Since 2007, Apache has posted at least 53 such security bulletins for Apache Struts.

32) Similarly, the U.S. Department of Commerce's National Institute of Standards and Technology ("NIST") maintains a free and publicly available National Vulnerability Database ("NVD") at http://nvd.nist.gov. Using the NVD, NIST identifies security vulnerabilities, including in open-source code, the risks they pose, and ways to fix them, including as to security vulnerabilities in Apache Struts.

33) Likewise, the MITRE Corporation, a "not-for-profit organization that operates research and development centers sponsored by the [United States] federal government," also identifies code security vulnerabilities, including vulnerabilities in Apache Struts, using a Common Vulnerabilities and Exposures ("CVE") Identifier. According to MITRE, the CVE Identifier is the industry standard for identifying publicly known cyber security vulnerabilities. MITRE maintains a database of CVE identifiers and the vulnerabilities to which they correspond, which is publicly accessible without cost online at https://cve.mitre.org (the "Vulnerability Database").

34) On March 7, 2017, Apache published notice of a security vulnerability in certain versions of Apache Struts in its online security bulletins S2-045 and S2-046 (the

"Apache Security Bulletins").[1] The vulnerability was assigned the CVE identifier CVE-2017-5638.

35) The Apache Security Bulletins were directed to "All Struts2 developers and users," and warned that the software was vulnerable to "Remote Code Execution," or "RCE." RCE refers to a method of hacking a public website whereby an online attacker can send computer code to the website that allows the attacker to infiltrate (that is, gain access to), and run commands on the website's server (the computer that stores the information that supports the website).

36) The Apache Security Bulletins assigned CVE-2017-5638 a "maximum security rating" of "critical." Apache recommended that users update the affected versions of Apache Struts to fix the vulnerability, or implement other specific workarounds to avoid the vulnerability.

37) NIST also publicized the March Security Vulnerability in its NVD on or about March 10, 2017 (the "NIST Notice").[2] NIST noted that the severity of the vulnerability was an overall score of 10.0 on two different versions of a scale called the Common Vulnerability Scoring System ("CVSS"). A score of 10.0 is the highest possible severity score on either scale. The NIST Notice also stated that an attack based on the vulnerability "[a]llow[ing] unauthorized disclosure of information," would be low in complexity to accomplish, and would not require the attacker to provide authentication (for example, a user name and password) to exploit the vulnerability.

---

[1] https://cwiki.apache.org/confluence/display/WW/S2-045 (last visited September 27, 2017). https://cwiki.apache.org/confluence/display/WW/S2-046 (last visited September 27, 2017).
[2] https://nvd.nist.gov/vuln/detail/CVE-2017-5638 (last visited September 27, 2017).

The NIST Notice also documented over twenty other website resources for advisories, solutions, and tools related to the March Security Vulnerability and how to patch or fix it.

38) Following the NIST Notice, the United States Computer Emergency Readiness Team ("US CERT") issued a security Bulletin (Bulletin (SB17-079)) on March 20, 2017, calling out the March Security Vulnerability as a "High" severity vulnerability ("US CERT Alert").[3]

39) In summary, as of or soon after March 7, 2017, Equifax knew or should have known, by virtue of multiple public sources, including all of the Apache Security Bulletins, the NIST Notice, the US CERT Alert, and the Vulnerability Database (as well as one or all of the various collateral sources referenced in the foregoing), that a security vulnerability existed in Apache Struts.

40) Other media reports have also identified other Equifax vulnerabilities within Equifax's online presence. Shortly following the Data Breach Disclosure, Hold Security, LLC began examining Equifax's South American operations and almost immediately discovered that an online portal designed to let Equifax employees in Argentina manage credit report disputes was easily hackable through information on Equifax's own web application. Specifically, a simple review of the open code on this web application would reveal the names, usernames, and passwords of these employees and allow anyone who simply knew how to look at this information access to 715 pages of information on users. Although at this point it is unclear whether this

[3] https://www.us-cert.gov/ncas/bulletins/SB17-079 (last visited September 27, 2017).

particular breach and lackadaisical approach to data security impacted U.S. consumers, it does reveal a particular propensity for Equifax to handle cavalierly the PII it has collected.

B. The Impact of the Data Breach

41) The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person." The FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[4]

42) Cybercriminals use personal information, such as that obtained by the cyberattackers that breached Equifax's data security systems, to commit a variety of identity-theft related crimes, including various types of government fraud such as: filing a fraudulent tax return; seeking immigration-related benefits; obtaining a driver's license or identification card in the victim's name but with another's picture; and/or using the victim's information to obtain government benefits.

43) Consumers spend hours of their own time and money repairing the damage caused by identity theft. According to the Department of Justice's Bureau of Justice Statistics

---

[4] Federal Trade Commission, Warning Signs of Identity Theft, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited September 27, 2017).

("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[5]

44) According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[6]

45) The Data Breach was a direct and proximate result of Equifax's failure to properly safeguard and protect Plaintiffs' and Class members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Equifax's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

46) Equifax had the resources to prevent a breach, but neglected to invest adequately in data security, despite the growing number of well-publicized data breaches. Had Equifax remedied the deficiencies in its data security systems, updated and corrected known security threats to regularly used applications, followed security guidelines, and adopted security measures recommended by experts in the field, Equifax would

---

[5] Victims of Identity Theft, 2014 (Sept. 2015) available at: http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited September 27, 2017).
[6] GAO, Report to Congressional Requesters, at p. 29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited September 27, 2017).

have prevented the Data Breach and, ultimately, the theft of Plaintiffs' and the Class's PII.

47) Equifax's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class members' PII, causing them to suffer economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information, including the imminent injury of potential identity theft by having their PII in the hands of cybercriminals and for sale on the dark Internet's black market;

b. unauthorized charges on their debit and credit card accounts;

c. unauthorized opening of credit lines and other loans in their names;

d. the failure to timely and adequately inform Plaintiffs and the Class of the Data Breach;

e. any ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

f. any ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the Data Breach;

g. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and,

h. the loss of productivity and value of their time spent to attempt to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

48) Plaintiffs and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII. As a direct and proximate result of Equifax's wrongful actions and inaction and the resulting Data Breach, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life pursuits to mitigate the actual and potential impact of the Data Breach on their daily lives including:

a. Seeking credit "freezes" with the CRAs;

b. Monitoring or closing accounts with financial institutions;

c. Obtaining and monitoring credit reports;

d. Purchasing or otherwise procuring credit monitoring services.

CLASS ALLEGATIONS

49) Plaintiffs seek relief on behalf of themselves and as representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a), (b)(2), (b)(3) and (c)(4), Plaintiffs seek certification of a Nationwide Class defined as follows:

> All persons residing in the United States whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Equifax in September 2017 (the "Nationwide Class").

50) Pursuant to Fed. R. Civ. P. 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs assert claims under the laws of the individual States, and on behalf of the separate statewide classes, defined as follows:

> All persons residing in North Carolina and/or Georgia whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Equifax in September 2017 (the "Statewide Classes").

51) Excluded from each of the above Classes are Equifax and any of its affiliates, parents or subsidiaries; all employees of Equifax; all persons who make a timely election to be excluded from the Class; government entities; and the judges to whom this case is assigned and their immediate family and court staff.

52) Plaintiffs hereby reserve the right to amend or modify the class definition with greater specificity or division after having had an opportunity to conduct discovery.

53) Each of the proposed Classes meets the criteria for certification under Federal Rule of Civil Procedure 23(a), (b)(2), (b)(3) and (c)(4).

54) **Numerosity**. Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is

impractical. Equifax has announced that it believes at least 143 million individuals whose PII was stolen as part of the Data Breach. Numerosity cannot reasonably be questioned given the size of the Data Breach in this case.

55) **Commonality**. Consistent with Rule 23(a)(2) and Rule 23(b)(3)'s predominance inquiry, this action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include:

a. Whether Equifax had a duty to protect PII;

b. Whether Equifax knew or should have known of the susceptibility of its data security systems to a data breach;

c. Whether Equifax's security measures to protect its systems were reasonable in light of the measures recommended by data security experts;

d. Whether Equifax was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Equifax's failure to implement adequate data security measures allowed the breach to occur;

f. Whether Equifax's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PII of Plaintiffs and Class members;

g. Whether Plaintiffs and Class members were injured and suffered damages or other unacceptable losses because of Equifax's failure to reasonably protect its data security network; and

h. Whether Plaintiffs and Class members are entitled to relief.

56) **Typicality**. Consistent with Rule 23(a)(3), Plaintiffs' claims are typical of those of other Class members. Plaintiffs had their PII compromised in the Data Breach. Plaintiffs' damages and injuries are akin to other Class members and Plaintiffs seek relief consistent with the relief of the Class.

57) **Adequacy**. Consistent with Rule 23(a)(4), Plaintiffs are adequate representatives of the Class because Plaintiffs are members of the Class and are committed to pursuing this matter against Equifax to obtain relief for the Class. Plaintiffs have no conflicts of interest with the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions, including privacy litigation. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class' interests.

58) **Superiority**. Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The present litigation involves a textbook example of the superior quality of a class action mechanism to resolve millions of claims in a single litigation that may otherwise be uneconomical to pursue in individual litigation. The burden and expense of litigating the present case in an individual capacity is comparatively high compared to the individual recovery of any individual Plaintiff or putative class member. Without the Rule 23 class mechanism, Plaintiffs and the Class would be without a practical path to remedy Equifax's wrongful conduct.

59) **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Equifax, through its uniform conduct, has acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and

declaratory relief appropriate to the Class as a whole. Equifax's former CEO claimed in public statements that Equifax has "more to do" to protect Plaintiffs' and the Class's PII and the Court should craft sufficient classwide injunctive relief to ensure that Equifax's data security systems comport with the law and industry standards.

60) Finally, all members of the proposed Class are readily ascertainable. Equifax has access to information regarding the Data Breach, the time period of the Data Breach, and which individuals were potentially affected. In fact, Equifax has established its own website to inform the public of whether they are affected by the Data Breach. Although problems with this website have been well documented in the media, the use of such a website indicates that Equifax itself knows or reasonably believes it knows, who the members of the class are. Using this information, the members of the Class can be identified and their contact information ascertained for purposes of providing notice to the Class.

COUNT I: NEGLIGENCE

On Behalf of Plaintiffs and the Nationwide Class, or, alternatively, Plaintiffs and the Separate Statewide Classes

61) Plaintiffs restate and reallege Paragraphs 1 through 60 as if fully set forth herein.

62) Upon accepting and storing Plaintiffs' and Class Members' PII in its computer systems and on its networks, Equifax undertook and owed a duty to Plaintiffs and Class Members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Equifax knew that the PII was private and confidential and should be protected as private and confidential.

63) Equifax owed a duty of care to Plaintiffs and the putative Class members to safeguard their PII because Plaintiffs and the putative Class members were foreseeable and probable victims of any cyberattack that successfully stole or obtained PII stored within Equifax's data security systems.

64) Equifax owed numerous duties to Plaintiffs and to members of the Nationwide Class, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting PII in its possession; and

b. to protect PII using reasonable and adequate security procedures and systems that are compliant with the law and industry-standard practices.

65) Equifax also breached its duty to Plaintiffs and the Class Members in that it failed to adequately protect and safeguard PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII. Furthering their dilatory practices, Equifax failed to provide adequate supervision and oversight of the PII with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted unknown cyberattackers to gather PII of Plaintiffs and Class Members, misuse the PII and intentionally disclose it to others without consent.

66) Equifax knew, or should have known, of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems, and the importance of adequate security. Equifax knew about numerous, well-publicized data breaches, including the

breach at Experian. Equifax knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiffs' and Class Members' PII.

67) Because Equifax knew that a breach of its systems would damage millions of individuals, including Plaintiffs and Class members, Equifax had a duty to protect its data systems and the PII contained therein.

68) Equifax's own conduct also created a foreseeable risk of harm to Plaintiffs and Class members and their PII. Equifax's misconduct included failing to: (1) secure its systems, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach. Specifically, Equifax had a duty to ensure that it timely updated its application to patch known security threats and knew or should have known that leaving known security threats open for only a few hours could provide cyberattackers enough time to breach Equifax's data systems. Any failure to timely patch these types of known data security threats is a gross deviation from the standard of care and routine, standard industry security practices.

69) Equifax breached its duties to Plaintiffs and Class members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII of Plaintiffs and Class members;

b. by failing to timely update or patch known security holes in the application Equifax routinely used in its normal course of business;

c. by creating a foreseeable risk of harm through the misconduct previously described;

d. by failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiffs' and Class members' PII both before and after learning of the Data Breach; and

e. by failing to comply with the minimum industry data security standards during the period of the Data Breach.

70) Through Equifax's acts and omissions described in this Complaint, including Equifax's failure to provide adequate security and its failure to protect PII of Plaintiffs and Class members from being foreseeably captured, accessed, disseminated, stolen and misused, Equifax unlawfully breached its duty to use reasonable care to adequately protect and secure PII of Plaintiffs and Class members during the time it was within Equifax possession or control.

71) Upon information and belief, Equifax improperly and inadequately safeguarded PII of Plaintiffs and Class Members in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Equifax's failure to take proper security measures to protect sensitive PII of Plaintiffs and Class members as described in this Complaint created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of PII of Plaintiffs and Class members.

72) Equifax's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect PII; failing to

conduct regular security audits; and failing to provide adequate and appropriate supervision of persons having access to PII of Plaintiffs and Class members.

73) Neither Plaintiffs nor the other Class members contributed to the Data Breach and subsequent misuse of their PII as described in this Complaint.

74) As a direct and proximate cause of Equifax's conduct, Plaintiffs and the Class suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the PII of Plaintiffs and Class Members; damages arising from Plaintiffs' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fee charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT II: VIOLATION OF THE NORTH CAROLINA AND GEORGIA STATE DATA BREACH STATUTES

On Behalf of Plaintiffs and the Separate Statewide Classes

75) Plaintiffs restate and reallege Paragraphs 1 through 74 as if fully set forth herein.

76) Equifax also had independent duties under state and federal laws that required Equifax to reasonably safeguard Plaintiffs' and Class members' PII and promptly notify them about the data breach.

77) The legislatures in North Carolina and Georgia have enacted state data breach statutes. See N.C. Gen. Stat. Ann. § 75-65(a), et seq.; Ga. Code Ann. § 10-1-912(a), et seq. These statutes generally require that any person or business conducting business within the state that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system to any resident of the state whose personal information was acquired by an unauthorized person. The statutes further require that the disclosure of the breach be made in the most expedient time possible and without unreasonable delay so that residents can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

78) The Equifax data breach constitutes a breach of the security system of Equifax within the meaning of the North Carolina and Georgia data breach statutes and the data breached is protected and covered by the below data breach statutes.

79) Plaintiffs' and Class Members' names, birth dates, Social Security numbers, credit card numbers, driver's license numbers, and documents pertaining to disputed charges

constitute personal information under and subject to the North Carolina and Georgia data breach statutes.

80) Equifax breached its duty to notify Plaintiffs and Class Members of the unauthorized access by waiting many months after learning of the breach to notify Plaintiffs and Class Members and then by failing to provide Plaintiffs and Class Members information regarding the breach until September 2017. Instead, its executives disposed of at least $1.8 million worth of shares in the company after Equifax learned of the data breach but before it was publicly announced. To date, Equifax has not provided sufficient information to Plaintiffs and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiffs and the Class.

81) Equifax failed to disclose to Plaintiffs and Class Members without unreasonable delay and in the most expedient time possible, the breach of security of Plaintiffs' and Class Members' personal and financial information when Equifax knew or reasonably believed such information had been compromised.

82) Through its failure to provide timely and clear notification of the Data Breach to consumers, Equifax prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their financial data and bank accounts.

83) Plaintiffs and Class Members suffered harm directly resulting from Equifax's failure to provide Plaintiffs and Class Members with timely and accurate notice as required by the North Carolina and Georgia data breach statutes.

84) Had Equifax provided timely and accurate notice of the data breach, Plaintiffs and Class Members would have been able to avoid and/or attempt to ameliorate or mitigate the damages and harm resulting in the unreasonable delay by Equifax in providing notice.

85) Plaintiffs and Class Members seek all remedies available under the North Carolina and Georgia data breach statutes, including but not limited to a) damages suffered by Plaintiffs and Class Members as alleged above, b) equitable relief, including injunctive relief, and c) reasonable attorney fees and costs, as provided by law.

COUNT III: NEGLIGENCE *PER SE*

On Behalf of Plaintiffs and the Nationwide Class, or, alternatively, Plaintiffs and the Separate Statewide Classes

86) Plaintiffs restate and reallege Paragraphs 1 through 85 as if fully set forth herein.

87) Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Equifax, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Equifax's duty in this regard.

88) Equifax violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Equifax's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data

breach at a corporation such as Equifax, including, specifically, the immense damages that would result to Plaintiffs and Class Members.

89) Equifax's violation of Section 5 of the FTC Act constitutes negligence *per se*.

90) Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

91) The harm that occurred as a result of the Equifax Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

92) As a direct and proximate result of Equifax's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, damages arising from Plaintiffs' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

COUNT IV: WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT ("FCRA")

On Behalf of Plaintiffs and the Nationwide Class, or, alternatively, Plaintiffs and the Separate Statewide Classes

93) Plaintiffs restate and reallege Paragraphs 1 through 92 as if fully set forth herein.

94) Plaintiffs and Class Members are consumers entitled to the protections of the FCRA. 15 U.S.C. § 1681a(c).

95) Under the FCRA, a "consumer reporting agency" is defined as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties . . . ." 15 U.S.C. § 1681a(f).

96) Equifax is a "consumer reporting agency" under the FCRA. As part of its standard business, for monetary fees, it regularly engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

97) As a consumer reporting agency, the FCRA requires Equifax to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a).

98) Under the FCRA, a "consumer report" is defined as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be

used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for -- (A) credit . . . to be used primarily for personal, family, or household purposes; . . . or (C) any other purpose authorized under section 1681b of this title." 15 U.S.C. § 1681a(d)(1). The compromised data was a consumer report under the FCRA because it was a communication of information bearing on Class members' credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living used, or expected to be used or collected in whole or in part, for the purpose of serving as a factor in establishing the Class members' eligibility for credit.

99) As a consumer reporting agency, Equifax may only furnish a consumer report under the limited circumstances set forth in 15 U.S.C. § 1681b, "and no other." 15 U.S.C. § 1681b(a). None of the purposes listed under 15 U.S.C. § 1681b permit credit reporting agencies to furnish consumer reports to unauthorized or unknown entities, or computer cyberattackers such as those who accessed the Nationwide Class members' PII. Equifax violated § 1681b by furnishing consumer reports to unauthorized or unknown entities or computer cyberattackers, as detailed above.

100) Equifax furnished the Nationwide Class members' consumer reports by disclosing their consumer reports to unauthorized entities and computer cyberattackers; allowing unauthorized entities and computer cyberattackers to access their consumer reports; knowingly and/or recklessly failing to take security measures that would prevent unauthorized entities or computer cyberattackers from accessing their consumer reports; and/or failing to take reasonable security measures that

would prevent unauthorized entities or computer cyberattackers from accessing their consumer reports.

101) The Federal Trade Commission ("FTC") has pursued enforcement actions against consumer reporting agencies under the FCRA for failing to "take adequate measures to fulfill their obligations to protect information contained in consumer reports, as required by the" FCRA, in connection with data breaches.

102) Equifax willfully and/or recklessly violated § 1681b and § 1681e(a) by providing impermissible access to consumer reports and by failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under § 1681b of the FCRA. The willful and reckless nature of Equifax's violations is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, Equifax touts itself as an industry leader in breach prevention; thus, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, and willingly failed to take them.

103) Equifax also acted willfully and recklessly because it knew or should have known about its legal obligations regarding data security and data breaches under the FCRA. These obligations are well established in the plain language of the FCRA and in the promulgations of the Federal Trade Commission. *See, e.g.*, 55 Fed. Reg. 18804 (May 4, 1990), 1990 Commentary on The Fair Credit Reporting Act. 16 C.F.R. Part 600, Appendix to Part 600, § 607 2E. Equifax obtained or had available these and other substantial written materials that apprised them of their duties under the FCRA. Any

reasonable consumer reporting agency knows or should know about these requirements. Despite knowing of these legal obligations, Equifax acted consciously in breaching known duties regarding data security and data breaches and depriving Plaintiffs and other members of the classes of their rights under the FCRA.

104) Equifax's willful and/or reckless conduct provided a means for unauthorized intruders to obtain and misuse Plaintiffs' and Nationwide Class members' personal information for no permissible purposes under the FCRA.

105) Plaintiffs and the Nationwide Class members have been damaged by Equifax's willful or reckless failure to comply with the FCRA. Therefore, Plaintiffs and each of the Nationwide Class members are entitled to recover "any actual damages sustained by the consumer . . . or damages of not less than $100 and not more than $1,000." 15 U.S.C. § 1681n(a)(1)(A).

106) Plaintiffs and the Nationwide Class members are also entitled to punitive damages, costs of the action, and reasonable attorneys' fees. 15 U.S.C. § 1681n(a)(2) & (3).

COUNT V: NEGLIGENT VIOLATION OF THE FCRA

On Behalf of Plaintiffs and the Nationwide Class, or, alternatively, Plaintiffs and the Separate Statewide Classes

107) Plaintiffs restate and reallege Paragraphs 1 through 106 as if fully set forth herein.

108) Equifax was negligent in failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. Equifax's negligent failure to maintain reasonable procedures is supported by, among other things, former employees' admissions that Equifax's data security

practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, as an enterprise claiming to be an industry leader in data breach prevention, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, yet failed to take them.

109) Equifax's negligent conduct provided a means for unauthorized intruders to obtain Plaintiffs' and the Nationwide Class members' PII and consumer reports for no permissible purposes under the FCRA.

110) Plaintiffs and the Nationwide Class members have been damaged by Equifax's negligent failure to comply with the FCRA. Therefore, Plaintiffs and each of the Nationwide Class member are entitled to recover "any actual damages sustained by the consumer." 15 U.S.C. § 1681o(a)(1).

111) Plaintiffs and the Nationwide Class members are also entitled to recover their costs of the action, as well as reasonable attorneys' fees. 15 U.S.C. § 1681o(a)(2).

COUNT VI: DECLARATORY JUDGMENT

On Behalf of Plaintiffs and the Nationwide Class, or, alternatively, Plaintiffs and the Separate Statewide Classes

112) Plaintiffs restate and reallege Paragraphs 1 through 111 as if fully set forth herein.

113) Plaintiffs and Class members entered into an implied contract that required Equifax to provide adequate security for the PII it collected from their payment card transactions. As previously alleged, Equifax owes duties of care to Plaintiffs and Class members that require it to adequately secure PII.

114) Equifax still possesses PII pertaining to Plaintiffs and Class members. Equifax has made no announcement or notification that it has remedied the vulnerabilities in its computer data systems, and, has publicly acknowledged that it "must do more" to secure the PII in its possession. Accordingly, Equifax has not satisfied its obligations and legal duties to Plaintiffs and Class members. In fact, now that Equifax's lax approach towards data security has become public, the PII in its possession is more vulnerable than previously.

115) Actual harm has arisen in the wake of the Equifax Data Breach regarding Equifax's contractual obligations and duties of care to provide data security measures to Plaintiffs and Class members.

116) Plaintiffs, therefore, seek a declaration that (a) Equifax's existing data security measures do not comply with its contractual obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Equifax must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis, and ordering Equifax to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. segmenting PII by, among other things, creating firewalls and access controls so that if one area of Equifax is compromised, cyberattackers cannot gain access to other portions of Equifax systems;

e. purging, deleting, and destroying in a reasonably secure manner PII not necessary for its provisions of services;

f. conducting regular database scanning and securing checks;

g. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Equifax customers must take to protect themselves.

COUNT VII: VIOLATION OF GEORGIA FAIR BUSINESS PRACTICES ACT O.C.G.A. § 10-1-390, *ET SEQ.*

On Behalf of Plaintiffs and the Nationwide Class

117) Plaintiffs restate and reallege Paragraphs 1 through 116 as if fully set forth herein.

118) Equifax is engaged in, and their acts and omissions affect, trade and commerce pursuant to O.C.G.A. § 10-1-392(28) ("GFBPA"). Equifax's acts, practices, and omissions at issue in this matter were directed and emanated from its headquarters in Atlanta, Georgia.

119) As alleged herein, Equifax engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including the following, in violation of the GFBPA:

a. failure to maintain adequate computer systems and data security practices to safeguard PII;

b. failure to disclose that its computer systems and data security practices were inadequate to safeguard PII from theft;

c. failure to timely and accurately disclose the Data Breach to Plaintiffs and Class members;

d. continued acceptance of PII and storage of other personal information after Equifax knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach; and

e. continued acceptance of PII and storage of other personal information after Equifax knew or should have known of the Data Breach and before it allegedly remediated the Breach.

120) Furthermore, as alleged above, Equifax's failure to secure consumers' PII violates the FTCA and therefore violates the GFBPA. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII of Plaintiffs and Class members, deter cyberattackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

121) As a direct and proximate result of Equifax's violation of the GFBPA, Plaintiffs and Class members suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were

fraudulently obtained through the use of the PII of Plaintiffs and Class Members; damages arising from Plaintiffs' inability to use their debit or credit cards or accounts because those cards or accounts were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

122) Also as a direct result of Equifax's knowing violation of the GFBPA, Plaintiffs and Class members are entitled to damages and injunctive relief, including, but not limited to:

a. Ordering that Equifax engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis, and ordering Equifax to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Equifax engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Equifax audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Equifax segment PII by, among other things, creating firewalls and access controls so that if one area of Equifax is compromised, cyberattackers cannot gain access to other portions of Equifax systems;

e. Ordering that Equifax purge, delete, and destroy in a reasonably secure manner PII not necessary for its provisions of services;

f. Ordering that Equifax conduct regular database scanning and securing checks;

g. Ordering that Equifax routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Equifax to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Equifax customers must take to protect themselves.

123) Plaintiffs bring this action on behalf of themselves and Class Members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiffs and Class members and the public from Equifax's unfair methods of competition and unfair, deceptive, fraudulent,

unconscionable and unlawful practices. Equifax's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

124) Plaintiffs and Class members are entitled to a judgment against Equifax for actual and consequential damages, exemplary damages and attorneys' fees pursuant to the GFBPA, costs, and such other further relief as the Court deems just and proper.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all Class members proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Equifax as follows:

1) For an Order certifying the Classes, as defined herein, and appointing Plaintiffs and their Counsel to represent the Nationwide Class, or in the alternative the separate Statewide Classes;

2) For equitable relief enjoining Equifax from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class members' PII, and from refusing to issue prompt, complete and accurate disclosures to the Plaintiffs and Class members;

3) For equitable relief compelling Equifax to use appropriate cyber security methods and policies with respect to consumer data collection, storage and protection and to disclose with specificity to Class members the type of PII compromised;

4) For an award of damages, as allowed by law in an amount to be determined;

5) For an award of attorneys' fees costs and litigation expenses, as allowable by law;

6) For prejudgment interest on all amounts awarded; and

7) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiffs demands a jury trial on all issues so triable.

This the 27th day of September, 2017.

s/ Katherine Langley
Katherine Langley
N.C. State Bar No. 22764
BURT LANGLEY, P.C.
149 S. Lexington Avenue
Asheville, NC 28801
Telephone: (828) 367-7090
Fax: (828) 318-8899
Email: klangley@burtlangley.com

J. Gerard Stranch, IV (TN BPR# 23045)
(PHV forthcoming)
Benjamin A. Gastel (TN BPR# 28699)
(PHV forthcoming)
Michael G. Stewart (TN BPR# 16920)
(PHV forthcoming)
BRANSTETTER, STRANCH & JENNINGS, PLLC
223 Rosa L. Parks Ave., Suite 200
Nashville, Tennessee 37203
(615) 254-8801
gerards@bsjfirm.com
beng@bsjfirm.com
mikes@bsjfirm.com

Attorneys for Plaintiffs